

## Freedom of Information Act 2000 (FOIA)

### Decision notice

**Date:** 15 February 2021

**Public Authority:** Chief Constable of West Yorkshire Police

**Address:** West Yorkshire Police  
PO Box 9  
Laburnum Road  
Wakefield  
WF1 3QP

### Decision (including any steps ordered)

---

1. The complainant requested information about police collar numbers. West Yorkshire Police ('WYP') provided some of the requested information but refused to provide the remainder, citing section 40(2) of the FOIA, the exemption for personal information.
2. The Commissioner's decision is that WYP was correct to rely on section 40(2) to withhold the remaining information for the reasons set out in this notice.
3. The Commissioner does not require WYP to take any steps to ensure compliance with the legislation.

### Request and response

---

4. On 24 February 2020, the complainant wrote to WYP and requested information in the following terms:

*"Q1. I would like to request the collar number of all West Yorkshire Police (WYP) Officers, broken down into either active or inactive Officers, where an inactive collar number is of Officers who may have left the force or the collar number is no longer used for other reasons.*

*Q2. For each collar number I would like to know the date the collar number became active and the date it was deactivated.*

*Q3. For each collar number I would like know how many officers have been allocated the same collar number over time or confirmation that once a collar number has been issued to an officer it is never reused and reactivated later through reassignment."*

5. WYP responded, late, on 24 July 2020 and provided the requested information for parts one and three of the request). It disclosed a report listing the requested collar numbers broken down by current and ex-officers. It refused to provide the information requested for part two of the request, citing section 40(2) of the FOIA, the exemption for personal information.
6. On 24 July 2020, the complainant requested an internal review in relation to part two only of his request. Following its internal review, WYP wrote to the complainant on 20 August 2020 and maintained that section 40(2) applied to part two.

### **Scope of the case**

---

7. The complainant contacted the Commissioner on 20 August 2020 to complain about the way his request for information had been handled.
8. He submitted the following grounds of complaint:

*"I believe the exemption being applied by the Force is incorrect. A police officer's Collar number along with the start and end date of said Collar number's usage does not constitute personal data as defined in the Data Protection Act (DPA) 2018, as the force seems to be now maintaining.*

*Given they have already provided the Collar numbers which the force accepts is not personal data then how can the extra pieces of data requested regarding start and end date of the Collar numbers usage in time now fall foul of the DPA legislation as personal data when the disclosure of the Collar number alone does not.*

*I believe the information requested does not constitute personal data, as an individuals [sic] work record is not personal data but business data. If, as in this case, the said business data happens to be one of a Public organisation such as a Police Force then all business data is subjected to the Freedom of Information legislation.*

*The exemption applied should therefore NOT be upheld."*

9. The Commissioner has considered whether WYP was entitled to rely on section 40(2) of the FOIA to withhold the information requested at part two of the request.

## **Reasons for decision**

---

### **Section 40 - personal information**

10. Section 40(2) of the FOIA provides that information is exempt from disclosure if it is the personal data of an individual other than the requester and where one of the conditions listed in section 40(3A)(3B) or 40(4A) is satisfied.
11. In this case the relevant condition is contained in section 40(3A)(a)<sup>1</sup>. This applies where the disclosure of the information to any member of the public would contravene any of the principles relating to the processing of personal data ('the DP principles'), as set out in Article 5 of the General Data Protection Regulation ('GDPR').
12. The first step for the Commissioner is to determine whether the withheld information constitutes personal data as defined by the Data Protection Act 2018 ('DPA'). If it is not personal data then section 40 of the FOIA cannot apply.
13. Secondly, and only if the Commissioner is satisfied that the requested information is personal data, she must establish whether disclosure of that data would breach any of the DP principles.

### ***Is the information personal data?***

14. Section 3(2) of the DPA defines personal data as:

*"any information relating to an identified or identifiable living individual".*

15. The two main elements of personal data are that the information must relate to a living person and that the person must be identifiable.
16. An identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

---

<sup>1</sup> As amended by Schedule 19 Paragraph 58(3) DPA.

17. Information will relate to a person if it is about them, linked to them, has biographical significance for them, is used to inform decisions affecting them or has them as its main focus.
18. In this case, the 'activation', and 'deactivation' dates for police collar numbers reflect WYP officers' start and end dates of employment with the force. WYP has explained that some police officer collar numbers were already in the public domain, such as neighbourhood officers, whereas the Commissioner understands that this will not always be the case, for example with covert officers. Disclosure of the service dates associated with a collar number could therefore reveal further details about a readily identifiable officer and be more intrusive.
19. WYP has told the Commissioner that:

*"The risk of identifying any individuals from just a collar number is very low especially as collar numbers are re-issued.*

*However for some officers, individual names are in the public domain alongside their collar numbers. Some officers names are in the public domain. Names and collar numbers of active police officers working in neighbourhood teams are listed on the WYP website. Example links below:<sup>2</sup>*

*Other officers, where necessary, will provide their names alongside their collar numbers to members of the public on a day to day basis – e.g. when working with vulnerable adults or children."*

20. Clearly, if the requested dates were to be released by WYP, any member of the public could 'marry up' any publicly available police officer collar numbers / names with the officer's start dates (and end dates where applicable). Furthermore, any member of the public who has dealt with a police officer may have been provided with their collar number as a necessary part of their interaction with the police, for example being arrested by an officer, being cautioned or in giving a statement. Disclosure would therefore allow these members of the public to also find out more details about an identified officer.
21. A test used by both the Commissioner and the First-tier Tribunal in cases such as this is to assess whether a 'motivated intruder' would be

---

<sup>2</sup> <https://www.westyorkshire.police.uk/my-neighbourhood/leeds/leeds-city/contacts>

<https://www.westyorkshire.police.uk/my-neighbourhood/bradford/bradford-city/contacts>

able to recognise an individual if he or she was intent on doing so. The 'motivated intruder' is described as a person who will take all reasonable steps to identify the individual or individuals but begins without any prior knowledge. In essence, the test highlights the potential risks of re-identification of an individual from information which, on the face of it, appears truly anonymised.

22. The ICO's Code of Practice on Anonymisation<sup>3</sup> notes that:

*"The High Court in [R (on the application of the Department of Health) v Information Commissioner [201] EWHC 1430 (Admin)] stated that the risk of identification must be greater than remote and reasonably likely for information to be classed as personal data under the DPA".*

23. In summary, the motivated intruder test is that if the risk of identification is "reasonably likely" the information should be regarded as personal data.

24. The Commissioner considers that a motivated intruder could potentially identify an WYP officer (or officers) through piecing together the now publicly available collar numbers with the associated 'activation' and 'deactivation' dates (if disclosed), together with other information known to them about an individual. There could be other data available that means re-identification by a third party is likely to take place and a member of the public who is trying to find out the length of service of an officer they have personally had dealings with could ascertain this from disclosure of the requested dates.

25. There are two main ways for re-identification to come about:

- An intruder takes personal data it already has and searches an anonymised dataset for a match.
- An intruder takes a record from an anonymised dataset and seeks a match in publicly available information.

26. Generally the latter risk scenario is of greater concern for data custodians because of the confidentiality pledges that are often given to those appearing in an anonymised dataset. However, both risk scenarios are relevant and can carry with them different probabilities of re-identification. In either case though, it can be difficult, even impossible, to assess risk with certainty.

---

<sup>3</sup> <https://ico.org.uk/media/fororganisations/documents/1061/anonymisation-code.pdf>

27. Despite all the uncertainty, re-identification risk can certainly be mitigated by ensuring that only the anonymised data necessary for a particular purpose is released. The fact that data has been anonymised does not mean that data minimisation techniques are not still relevant.
28. In the circumstances of this case, having considered the withheld information, the Commissioner is satisfied that the information relates to both serving and former WYP officers. She is satisfied that this information both relates to, and potentially identifies information about, those officers. Where the officers' collar numbers and names are already in the public domain (as is the case on the websites highlighted by WYP), release of the requested dates would reveal those officers' employment start dates (and potentially end dates in some cases). This information therefore falls within the definition of 'personal data' in section 3(2) of the DPA.
29. Additionally, the Commissioner must give consideration to the 'motivated intruder' and the risk of re-identification of those officers whose names are not already publicly available, together with their employment start (and end where applicable) dates. This would include those collar numbers which are personally known to members of the public where they have necessarily been provided for policing purposes whereas they would not generally be disclosed to the world at large. This information therefore also falls within the definition of 'personal data' in section 3(2) of the DPA.
30. The fact that information constitutes the personal data of an identifiable living individual does not automatically exclude it from disclosure under the FOIA. The second element of the test is to determine whether disclosure would contravene any of the DP principles.
31. The most relevant DP principle in this case is principle (a).

### **Would disclosure contravene principle (a)?**

32. Article 5(1)(a) of the GDPR states that:

*"Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject".*

33. In the case of an FOIA request, the personal data is processed when it is disclosed in response to the request. This means that the information can only be disclosed if to do so would be lawful, fair and transparent.
34. In order to be lawful, one of the lawful bases listed in Article 6(1) of the GDPR must apply to the processing. It must also be generally lawful.

### **Lawful processing: Article 6(1)(f) of the GDPR**

35. The Commissioner considers that the lawful basis most applicable is basis 6(1)(f) which states:

*"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child"<sup>4</sup>.*

36. In considering the application of Article 6(1)(f) of the GDPR in the context of a request for information under the FOIA, it is necessary to consider the following three-part test:-

- i) **Legitimate interest test:** Whether a legitimate interest is being pursued in the request for information;
- ii) **Necessity test:** Whether disclosure of the information is necessary to meet the legitimate interest in question;
- iii) **Balancing test:** Whether the above interests override the legitimate interest(s) or fundamental rights and freedoms of the data subject.

37. The Commissioner considers that the test of 'necessity' under stage (ii) must be met before the balancing test under stage (iii) is applied.

#### *Legitimate interests*

38. In considering any legitimate interest(s) in the disclosure of the requested information under FOIA, the Commissioner recognises that a wide range of interests may be legitimate interests. They can be the

---

<sup>4</sup> Article 6(1) goes on to state that:-

*"Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks".*

However, section 40(8) FOIA (as amended by Schedule 19 Paragraph 58(8) DPA) provides that:-

*"In determining for the purposes of this section whether the lawfulness principle in Article 5(1)(a) of the GDPR would be contravened by the disclosure of information, Article 6(1) of the GDPR (lawfulness) is to be read as if the second sub-paragraph (dis-applying the legitimate interests gateway in relation to public authorities) were omitted".*

requester's own interests or the interests of third parties, and commercial interests as well as wider societal benefits. These interest(s) can include broad general principles of accountability and transparency for their own sakes, as well as case-specific interests. However, if the requester is pursuing a purely private concern unrelated to any broader public interest, unrestricted disclosure to the general public is unlikely to be proportionate. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test.

39. The complainant has not submitted any legitimate interest arguments *per se* and has instead argued that disclosure of the 'activation' and 'deactivation' dates of WYP's police collar numbers does not constitute personal data; the Commissioner does not agree for the reasons given above.
40. WYP has recognised the legitimate interests of the complainant/public in asking a public body whether it holds information and to ask for a copy of information held.
41. The Commissioner cannot identify any particular legitimate interests in the provision of the 'activation' and 'deactivation' dates of the disclosed collar numbers, other than acknowledging that this is of some undefined interest to the complainant himself.

*Is disclosure necessary?*

42. 'Necessary' means more than desirable but less than indispensable or absolute necessity. Accordingly, the test is one of reasonable necessity and involves consideration of alternative measures which may make disclosure of the requested information unnecessary. Disclosure under the FOIA must therefore be the least intrusive means of achieving the legitimate aim in question.
43. In the circumstances of this case, the Commissioner notes that WYP has attempted to meet its legitimate interest obligations to openness and transparency under the FOI by the disclosure of some of the requested information.
44. The complainant has not submitted any reason(s) why the provision of the 'activation' and 'deactivation' dates for the disclosed collar numbers is "*necessary*".
45. WYP submitted the following:

*"WYP has confirmed that it holds the information and has confirmed that collar numbers can be re-assigned. Whilst the public may desire the information about an officer's dates of service it is not absolutely necessary for this information to be placed into the public domain."*



*Where a member of the public requires the information for a lawful purpose there [sic] other less intrusive routes to the information available to the public. For example, if the public wishes to make a complaint about an officer (past or present) they may do so by contacting PSD [Professional Standards Department) and providing either a crime reference number or officer name of [sic] officer collar number. If the information is relevant to the outcome of the complaint it may be lawfully disclosed. This allows disclosure to be considered on a case by case basis and enables the Chief Constable to consider what is necessary, relevant and a proportionate for disclosure and ensure that he is able to respects the rights and freedoms of the data subjects. Whereas disclosure under FOIA is the most intrusive means of achieving the legitimate aim."*

46. The Commissioner accepts that it is not "necessary" for an officer's dates of service with WYP to be in the public domain. She cannot see any value in that information being publicly released *en masse* and no rationale has been provided by the complainant. However, she can see where length of service could potentially be used to the detriment of an officer, in that the public, and more importantly criminals, could identify officers with shorter service and, by association, less experience, which they may try to use to their advantage.
47. As the Commissioner has decided in this case that disclosure is not necessary to meet the legitimate interest in disclosure, she has not gone on to conduct the balancing test. As disclosure is not necessary, there is no lawful basis for this processing and it is unlawful. It therefore does not meet the requirements of principle (a).

### *Conclusion*

48. The Commissioner has therefore decided that WYP was entitled to withhold the information requested at part two of the request, under section 40(2), by way of section 40(3A)(a).

## **Right of appeal**

---

49. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

First-tier Tribunal (Information Rights)  
GRC & GRP Tribunals,  
PO Box 9300,  
LEICESTER,  
LE1 8DJ

Tel: 0300 1234504

Fax: 0870 739 5836

Email: [grc@justice.gov.uk](mailto:grc@justice.gov.uk)

Website: [www.justice.gov.uk/tribunals/general-regulatory-chamber](http://www.justice.gov.uk/tribunals/general-regulatory-chamber)

50. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.
51. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

**Signed .....**

**Carolyn Howes**  
**Senior Case Officer**  
**Information Commissioner's Office**  
**Wycliffe House**  
**Water Lane**  
**Wilmslow**  
**Cheshire**  
**SK9 5AF**